UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA

MEMORANDUM AND ORDER
23-CR-192 (NRM)

-against-

JASON ROBINSON,

Defendant.

----------x

NINA R. MORRISON, United States District Judge:

Pending before the Court is Defendant Jason Robinson's motion to suppress evidence obtained by the government (1) during Robinson's detention and manual search of his iPhone at JFK Airport (2) thereafter through a warrant issued for a forensic search of the same cell phone. The Court has considered the parties' written briefs, the testimony given and exhibits entered at the suppression hearing held on January 8, 2025, the parties' statements from oral argument held on January 15, 2025, and all other letters and briefs submitted to the Court. For the reasons outlined below, Robinson's motion is GRANTED.

## OVERVIEW

On November 14, 2022, Jason Robinson, a resident of Pennsylvania and a United States citizen, returned from a vacation in Egypt with his spouse. At customs, he was detained at secondary inspection at John F. Kennedy International Airport ("JFK"), and directed to hand over and provide the passwords to his electronic devices. A Customs and Border Patrol ("CBP") agent manually searched his cell phone and

found evidence of child pornography. Relying on that information, a Special Agent from Homeland Security Investigations ("HSI") seized all of Robinson's devices and thereafter applied for a warrant to conduct a forensic search of Robinson's phone. After additional pictures and videos depicting child pornography were found as a result of the forensic search, Robinson was indicted on one count of Transportation of Child Pornography, in violation of 18 U.S.C. § 2252(a)(1), and one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

Robinson now seeks to suppress the contents of his cell phone. In support of his motion to suppress the physical evidence, Robinson argues that the Fourth Amendment requires the search of a cellular device at the border to be supported by a warrant and probable cause — neither of which was present here. This Court agrees. Although the Second Circuit has yet to address this issue, the Court has previously considered it in *United States v. Sultanov*, 742 F. Supp. 3d 258 (E.D.N.Y. 2024), where it determined that the search of a cellular device at the border must indeed be supported by a warrant and probable cause.

Additionally, the Court does not find that the search of Robinson's phone at JFK, or the subsequent forensic search pursuant to a warrant, are covered by the good faith exception to the exclusionary rule. As detailed below, this is chiefly because (1) the limited information that led CBP to search Robinson's cell phone at JFK airport did not provide reasonable suspicion that he possessed contraband on his device at the time of the search, and (2) the Special Agent who prepared the subsequent warrant application misled the magistrate judge about the actual

circumstances that led to the airport search, intentionally omitting the one and only item of specific information known to CPB that led Robinson to be targeted for secondary screening and a device search in the first place. Thus, because the warrantless searches of Robinson's phone violated the Fourth Amendment and are not covered by any exceptions to the warrant requirement or the exclusionary rule, Robinson's motion to suppress the contents of his cell phone is GRANTED.

## FACTS AND PROCEDURAL HISTORY

The Court makes the following findings of fact based on the testimony and evidence presented at a suppression hearing held in this case and in exhibits offered by both parties.

### I. Background Facts

#### A. Initial Search of Robinson's Phone

On November 14, 2022, Jason Robinson arrived at JFK Airport aboard a British Airways flight from London, United Kingdom, which originated in Cairo, Egypt. *See* Warrant Aff., Def. Mot. to Suppress Ex. C, ECF 25-5 ¶ 7. Robinson was traveling with his spouse, and returning from his first trip ever outside of the country. *See* Transcript of January 8, 2025 Suppression Hearing ("Hr'g Tr.") at 52. As Robinson went through customs, he was asked routine questions about his identity and travel itinerary by an officer. *See* Robinson Decl., Def. Mot. to Suppress Ex. A, ECF 25-3 at 1. The officer then brought Robinson, without his spouse, to a separate room where he was called to a counter and asked questions by a different, female officer. *Id.* at 1–3. He was asked by that officer what electronic devices he was

carrying, and he produced his iPhone, a laptop, and a Nintendo Switch gaming device. *Id.* at 2.

That second officer was Customs and Border Patrol ("CBP") Officer Shahamin Nunes. *See* Hr'g Tr. at 20–21, 41. On November 14, 2022, Officer Nunes was assigned as a secondary officer at JFK Terminal 7. *See id.* at 22. A secondary officer conducts a "secondary inspection," which occurs after the initial officer, to whom an individual presents their passport, refers a passenger to "a special room" where the secondary inspection is conducted. *Id.* at 23. Officer Nunes confirmed that Robinson's spouse was not allowed in the room for the secondary inspection. *Id.* at 47–48.

The secondary room to which Robinson was directed consists of around 40 to 50 chairs which all face a long bench where the secondary officers sit. *Id.* at 27. The room is approximately 50 or 40 feet by 40 or 30 feet. *Id.* Although the doors to the room remain open, Officer Nunes confirmed that Robinson was not free to "leave until [his] inspection[] [was] over." *Id.* at 86.

The primary officer referred Robinson to secondary inspection because the information presented was considered a "mandatory referral." *Id.* at 46. This information was in the form of a "TECS lookout."[1] *See* TECS Report, Gov't Hr'g Ex. 101. The TECS report, which Officer Nunes reviewed before speaking to Robinson, read: "Subj linked to the purchase of child sexual exploitation material via FinCen. Refer to secondary for interview & media device exam to include cell phones and

[1] The government indicates that TECS is not an acronym but rather is the "name for a system formerly known as the Treasury Enforcement Communications System." Gov't Opp., ECF 27 at 8 n.2.

laptops." *Id.* at 2; Hr'g Tr. at 45–47. This TECS lookout for Robinson was entered on November 11, 2019 — three years before Robinson's arrival at JFK. *Id.* at 1; Hr'g Tr. at 50.

Officer Nunes then called Robinson up and asked him a few preliminary questions. He answered her questions fully and told her that he was traveling from Egypt with his spouse. Hr'g Tr. at 47. All of Robinson's answers to these preliminary questions, such as whether he had any friends or family in Egypt, the purpose of the travel, and what he did for work, "matched" what Officer Nunes had in her system and, insofar as she was aware, appeared to be truthful. *Id.* at 80–82.

Officer Nunes then gave Robinson a "tear sheet" which "explain[ed] CBP's authority to search electronic devices." *Id.* at 53–54; *see also* Tear Sheet, Gov't Hr'g Ex. 102. She told him that CBP had the authority to conduct an exam. Hr'g Tr. at 52. She then directed him to provide her with the passwords to his phone and other electronic devices. *Id.* at 54. He provided them, and she wrote them down on a sticky note. *See id.* at 56.

Officer Nunes testified that if Robinson had refused to give her the devices or the passwords to them, she would have had "to contact [her] supervisor and see how they would want to proceed." *Id.* at 55–56, 79. However, in the approximately 50 electronic device searches that she has conducted, she has never once had a passenger refuse to hand over their devices. *Id.*

Officer Nunes then put Robinson's laptop in airplane mode, so it would not connect to the internet, and searched it for evidence of child sexual exploitation/abuse

material ("CSEM" or "CSAM"). *Id.* at 59. Robinson stayed seated in front of her at her desk as she performed a roughly thirty-minute search of his laptop, but found no evidence of CSAM. *See id.* at 60–61.

After that, she proceeded to search Robinson's iPhone. *Id.* at 61. After roughly 15 minutes of searching applications on Robinson's phone, Officer Nunes viewed videos and photographs that appeared to be depictions of CSAM in a folder called "My Favorites." *Id.* at 62–63. At that point, Officer Nunes alerted Homeland Security Investigations ("HSI"). *Id.* at 64.

About an hour later, HSI agent Allen Anstee arrived, and he took the devices into a separate room. *Id.* at 65–66. Agent Anstee conducted a brief review of Robinson's iPhone, and also observed CSAM. Gov't Opp. at 9–10. Agent Anstee then called Robinson into the interview room, where Anstee interviewed Robinson. *Id.* at 10. Robinson was not arrested that night and was allowed to leave the airport. Hr'g Tr. at 66. However, HSI retained possession of his electronic devices. *Id.*

**B. Search Warrant**

That same day, Agent Anstee called HSI Agent Richard Stepien. *Id.* at 136–37. Agent Anstee relayed to Agent Stepien that he had identified CSAM on Robinson's phone after a manual search of the phone at JFK airport. *Id.* at 137. Agent Stepien also reviewed the reports from the CBP Officers involved in the initial search. *Id.* Agent Stepien knew, from those reports, that Robinson had specifically been referred to secondary inspection because of a TECS report. *Id.* at 146.

One week later, on November 21, 2022, Agent Stepien applied for a warrant to search Robinson's seized phone. *Id.* at 138–39; Warrant Aff. at 12. Although HSI had already identified CSAM on the phone, Agent Stepien testified that he applied for a warrant to search that same device "out of an abundance of caution because we were hoping to do a more thorough examination of the phone that is not as easily done manually." *Id.* at 138.

In the warrant application, Stepien described the circumstances that led to the seizure of Robinson's phone as follows:

> [] On November 14, 2022, ROBINSON landed at John F. Kennedy International Airport ("JFK Airport"), traveling from Cairo, Egypt, via British Airways flight BA 115 arriving from London, United Kingdom. He was stopped by United States Customs and Border Protection ("CBP") at JFK Airport for secondary inspection. A border search was conducted. During the search, ROBINSON voluntarily gave CBP officers the password for the Subject Device. Upon manually reviewing the Subject Device, CBP officers identified that there was child sexual abuse material on the subject device.
>
> [] At the border, a law enforcement agent with HSI conducted a preliminary review of the Subject Device and confirmed that it contained at least five photos containing child sex abuse material.

Warrant Aff. ¶¶ 7–8.

After the sentence "[a] border search was conducted," Agent Stepien added a footnote that read: "The federal government has 'broad plenary powers to conduct so-called "routine" searches at the border even without "reasonable suspicion that the prospective entrant has committed a crime."'" *Id.* at 3 n.1 (quoting *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015)). Agent Stepien also indicated that following the initial search by CBP, an HSI agent reviewed the phone and confirmed that it

contained "at least five photos containing child sex abuse material." *Id.* ¶ 8. Magistrate Judge Cho granted the application and signed the warrant that same day. *Id.* at 12.

### C. The Subsequent Searches and Interview

Following the issuance of the warrant, Agent Stepien conducted a forensic examination of the phone, revealing 235 images that were classified as CSAM. Hr'g Tr. at 141. The examination also revealed 457 videos classified as CSAM. *Id.*

On January 17, 2023, Agent Stepien applied for a warrant to search the remaining devices they had seized from Robinson, including a laptop, a USB thumb drive, and a memory card. Gov't Opp. at 12. Agent Stepien based the probable cause determination in that warrant application on the photos and videos that had been recovered from Robinson's phone. *Id.* That warrant was also authorized, and the search of Robinson's remaining devices revealed 21 images and four videos containing CSAM. *Id.*

On May 1, 2023, a Grand Jury returned an indictment charging Robinson with the Transportation of Child Pornography, in violation of 18 U.S.C. § 2252(a)(1), and Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). *See* Indictment, ECF No. 1. On May 16, 2023, Agent Stepien arrested Robinson. *See* Hr'g Tr. at 147. Robinson agreed to speak with investigators after being advised of his *Miranda* rights, acknowledging that CSAM was present on his phone. Gov't Opp. at 12–13.

## II. Procedural History

On July 10, 2024, Robinson filed the instant motion to suppress. *See* Robinson Br., ECF No. 25 at 1. Specifically, he asserted that the initial search and seizure of his phone at JFK airport by CBP and subsequently by HSI violated his Fourth Amendment rights, as the border-search exception to the warrant requirement does not permit the warrantless search of a traveler's cell phone; that the officers lacked not only probable cause, but even reasonable suspicion to believe that he was traveling in possession of contraband. *Id.* at 9–17. He also argued that any statements made to Agent Anstee on the day of the search should be suppressed under the Fifth Amendment, arguing that he was in custody by the time the interview was conducted and that he was not advised of his *Miranda* rights. *Id.* at 17–21. Lastly, he claimed that the government had unreasonably delayed its application for a warrant to search the laptop, SD card, and thumb drive despite seizing those devices nine weeks earlier, was unreasonable, and that the evidence obtained from those searches should therefore be suppressed as well. *Id.* at 22–24.

Regarding the search of Robinson's iPhone, the government argued that the warrantless search at JFK Airport was covered by the border search exception, permitting CBP to conduct a device search without any individualized suspicion at all. Gov't Opp. at 14–21. It then contended, alternatively, that even if a border search of a traveler's cell phone requires reasonable suspicion, the November 2019 TECS report in this case provided the requisite reasonable suspicion. *Id.* at 21–23. Last, the government argued that even if probable cause and a warrant are required, the

fruits of the search should not be suppressed because the officers conducting it were covered by the good faith exception to the exclusionary rule. In the government's view, the good faith exception applies because (1) the initial search was done in reliance on Second Circuit and Supreme Court precedent that authorizes a search of traveler's phone as "routine"; (2) alternatively, even a "nonroutine" search need only be supported by reasonable suspicion, which the CBP officer had in this case; and (3) because the subsequent forensic search was done in reasonable reliance on Judge Cho's warrant. *Id.* at 23–27.

The Court scheduled an evidentiary hearing to take place on January 8, 2025. *See* Order dated on Nov. 12, 2024. On December 27, 2024, the government filed a letter with the Court, narrowing the claims at issue and arguing that a hearing was unnecessary. *See* Gov't Letter Dated Dec. 27, 2024, ECF No. 38 (Gov't 12/27/2024 Ltr.). First, the government proffered that it will not seek to admit at trial any of the evidence recovered from any of Robinson's devices besides his iPhone. *Id.* at 1. The government also stated that it did not intend to offer any of Robinson's statements made to Agent Anstee on November 14, 2022. *Id.* at 2 n.1. The government then argued that all of the remaining issues were legal, not factual, and therefore an evidentiary hearing was unnecessary. *Id.* at 2–3.

The Court denied the government's request to cancel the evidentiary hearing. *See* Docket Order on 1/2/2025. However, based on the government's representations that certain aspects of the motion were now moot, the Court denied without prejudice the aspects of Robinson's motion that related to his statements to Agent Anstee and

the evidence recovered from any device other than his iPhone. *See* Minute Entry on 1/8/2025.

At the evidentiary hearing, the government put on three witnesses: CBP Officer Shahamin Nunes, Special Agent Egbert Simon of the United States Attorney's Office (formerly of CBP), and Special Agent Richard Stepien. *See id.* The Court then held oral argument one week later, on January 15, 2025. *See* Minute Entry on 1/15/2025.

## DISCUSSION

On a motion to suppress in a criminal case, the defendant bears the burden of demonstrating the basis for the motion. *See United States v. Masterson*, 383 F.2d 610, 614 (2d Cir. 1967). Once the defendant meets his burden, the burden shifts to the government. *See United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980). Where the defendant's motion is premised on a Fourth Amendment violation, "the Government bears the burden of justifying an exception to the warrant requirement by a preponderance of the evidence." *United States v. Alisigwe*, No. 22-cr-425 (VEC), 2023 WL 8275923, at *4 (S.D.N.Y. Nov. 30, 2023) (citing *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980)).

### I. Fourth Amendment

The Fourth Amendment to the Constitution protects "[t]he right of the people to be secure . . . against unreasonable searches and seizures." U.S. Const. amend. IV. The Fourth Amendment "expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless

probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011).

Before law enforcement officers conduct a search for evidence of a crime, "reasonableness generally requires the obtaining of a judicial warrant," subject to several narrowly delineated exceptions. *Riley v. California*, 573 U.S. 373, 382 (2014) (internal quotation marks omitted). This case implicates the so-called "border exception" to the warrant requirement, which has historically been applied to exempt government officials from the warrant requirement and allow them to conduct brief searches of travelers' persons and effects to prevent contraband from entering the country. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). The issue here is whether, in light of that exception, a compelled search of the contents of a traveler's cell phone or other handheld electronic device conducted without a warrant and without probable cause is reasonable under the Fourth Amendment if that search takes place at an international border.[2] If the Court answers that question in the negative, then the warrantless search of Robinson's cell phone violated the Fourth Amendment, and the fruits of that search could be subject to suppression.

### A. The Warrant Exception for Routine Border Searches

When assessing the reasonableness of a search, courts are guided by "balancing its intrusion on the individual's Fourth Amendment interests against its

[2] An international airport, like JFK, "is considered the functional equivalent of a border for Fourth Amendment purposes." *Alisigwe*, 2023 WL 8275923, at *3 n.5 (internal quotation marks omitted).

promotion of legitimate governmental interests." *Montoya de Hernandez*, 473 U.S. at 537 (internal quotation marks omitted). At the border, searches that would violate the Fourth Amendment if they were conducted within the country may be reasonable because the balance between the government's interests and the individual's privacy interests tips decidedly in the government's favor. *See id.* at 539–40. That is because the government's "interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). And a traveler in an international airport seeking entry into the United States has a diminished expectation of privacy due in part to the surveillance and security measures that are endemic in air travel. *See Montoya de Hernandez*, 473 U.S. at 539–40.

The border search exception is based not only on the "balance between the interest of the Government and the privacy right of the individual," which is "struck much more favorably to the Government at the border," but also on the history and tradition of the government's customs enforcement power. *Id.* at 537–40. The same Congress that proposed the Bill of Rights enacted the first customs statute that empowered customs officials to search incoming "ship[s] [and] vessel[s]" suspected of transporting "any goods, wares or merchandise subject to duty." *United States v. Ramsey*, 431 U.S. 606, 616 (1977) (internal quotation marks omitted).

Although such searches, if conducted domestically, would have required a warrant and probable cause to be reasonable under the Fourth Amendment, those warrantless searches by customs officials were reasonable "simply by virtue of the

fact that they occur[red] at the border." *Id.*; *see also United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) ("Customs officers characteristically inspect luggage and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country."). The historic power of customs officials to conduct "routine inspections and searches" of goods at the border and "its functional equivalents" also extends to searches of people at the border based on the government's power "to exclude aliens from the country." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973). Thus, for at least two centuries, the government's "inherent authority to protect" and "paramount interest in protecting[] its territorial integrity," *Flores-Montano*, 541 U.S. at 153, has led courts to uphold searches of people and property at the border that would under ordinary circumstances violate the Fourth Amendment. *See Montoya de Hernandez*, 472 U.S. at 554 (Brennan, J., dissenting) (distinguishing between searches at the border "*for purposes of immigration and customs control*" and searches "carried out *for purposes of investigating suspected criminal activity*").

**B. Nonroutine Searches at the Border**

"Nonetheless, the touchstone of the Fourth Amendment analysis remains reasonableness," and the border search exception "does not mean . . . that at the border anything goes." *United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013) (internal quotation marks omitted). The Supreme Court has differentiated between routine border searches, like the search of a traveler's luggage, *see Thirty-Seven Photographs*, 402 U.S. at 376, and searches conducted at the border "for purposes

other than a routine border search" that exceed the "scope of a routine customs search and inspection," *see Montoya de Hernandez*, 473 U.S. at 540–41. "[T]he level of intrusion into a person's privacy is what determines whether a border search is routine" and thus whether the border search exception applies or not. *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006).

To determine whether a warrantless, nonroutine search is permissible under the Fourth Amendment, courts conduct the customary reasonableness balancing test, in which "the offensiveness of the intrusion must be weighed against the level of warranted suspicion." *Id.* For example, in *Montoya de Hernandez*, the Supreme Court held that a noncitizen traveler who presented herself for admission at the border and was suspected of "smuggling contraband in her alimentary canal" was lawfully detained by CBP for sixteen hours because CBP had reasonable suspicion that the traveler was attempting to smuggle drugs into the country, and because they detained her only "for the period of time necessary to either verify or dispel" the suspicion. 473 U.S. at 541–44. The Court considered the totality of the circumstances surrounding the traveler's detention and weighed the intrusiveness of the detention at issue against the government's "longstanding concern for the protection of the integrity of the border." *Id.* at 538. And the government's interest in taking reasonable measures to interdict the flow of illegal narcotics was, in the Court's view, entitled to great weight given what was, at that time, a "veritable national crisis in law enforcement caused by smuggling of illicit narcotics." *Id.*

Similarly, in *United States v. Asbury*, 586 F.2d 973 (2d Cir. 1978), the Second Circuit assessed the Fourth Amendment reasonableness of a strip search at the border of a traveler suspected of carrying contraband. The court characterized the challenged strip search as a nonroutine search not governed by the border search exception, reasoning that while "anyone entering or leaving the country may expect to have his luggage and personal effects examined, he does not expect that his entry or departure, standing alone, will cause him to be subjected to a strip search." *Id.* at 975. The court then conducted the traditional Fourth Amendment reasonableness analysis in the specific (border-security) context presented. *Id.* at 976–77. It weighed the traveler's expectation of privacy against the government's heightened interest in preventing illegal narcotics from being smuggled across the border and ultimately upheld the search as supported by individualized suspicion and within the Fourth Amendment's bounds of reasonableness. *Id.*; *see also Irving*, 452 F.3d at 123 (citing *Asbury*, 586 F.2d at 975–76, for the proposition that while "routine border searches of a person's belongings," including searches of "outer clothing, luggage, a purse, wallet, pockets, or shoes," "are made reasonable by that person's decision to enter this country, more invasive searches, like strip searches" that "substantially infringe on a traveler's privacy rights," "require reasonable suspicion").

### C. A Warrant is Required for the Search of a Cell Phone at the Border

To date, neither the Supreme Court nor the Second Circuit has decided (1) whether a search of a traveler's cell phone or other handheld electronic device at the border is a routine search covered by the border search exception, or (2) if it is a

nonroutine search, the level of suspicion required for the search to be reasonable under the Fourth Amendment (*i.e.,* whether it may be conducted at the point of entry by border officials based on a mere showing of reasonable suspicion or whether it requires a warrant and probable cause).

However, a number of district courts in this Circuit have had the issue squarely presented to them in border-search challenges in recent years. In one such case, this Court reviewed the Supreme Court's and Second Circuit's related jurisprudence and concluded that the search of a cell phone at the border, whether a so-called "manual" or "forensic" search, is a nonroutine search. *See United States v. Sultanov*, 742 F. Supp. 3d 258, 288 (E.D.N.Y. 2024). In that same case, this Court further held that applying that existing caselaw, including but not limited to the Supreme Court's decision in *Riley,* to the cell phone context compels the conclusion that the Fourth Amendment requires probable cause and a warrant for the government to search a traveler's cell phone. *See id.* at 296 ("Where the government seeks access to private devices that hold such a vast array of expressive content [such as cell phones], only the standard conceived by the Founders and codified in the Fourth Amendment — probable cause and the approval of a neutral magistrate — can bear the weight of that obligation.").

The Court's reasoning is more fully detailed in *Sultanov* itself, *see id.* at 280–96, but given that both parties have raised the issue anew in this motion, it is summarized below.

The Court begins its analysis with the Supreme Court's 2014 decision in *Riley v. California*, where the Court addressed how the search incident to arrest exception to the warrant requirement applies to modern cell phones. 573 U.S. at 385. In *Riley*, the Court concluded that "[c]ell phones differ in both a quantitative and qualitative sense from other objects" an arrestee might have on their person because they are "in fact minicomputers" with "immense storage capacity" that allowed an individual to carry "every piece of mail they have received in the past several months, every picture taken, [and] every book or article that they have read." *Id.* at 393–94. The Court explained that "a cell phone search would typically expose to the government far *more* [information] than the most exhaustive search of a house." *Id.* at 396–97. The Court concluded that because modern cell phones "hold for many Americans the privacies of life," the "answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple — get a warrant." *Id.* at 403 (internal quotation marks omitted).

Following *Riley*, the Second Circuit has recognized the immense privacy concerns implicated by the search of electronic devices. *See United States v. Smith*, 967 F.3d 198, 208 (2d Cir. 2020) ("[T]he search and seizure of personal electronic devices like a modern cell phone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person's ordinary personal effects."). The Circuit has noted that it is not just the *quantity* of the data contained on an electronic device which triggers heightened privacy concerns, but also the nature of that material, explaining that in *one* place the government can find "[t]ax

records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, [and] banking and shopping information." *United States v. Ganias*, 824 F.3d 199, 218 (2d Cir. 2016) (en banc).

While it is true that *Riley* concerned the search incident to arrest exception to the warrant requirement, the Supreme Court's clear holding regarding the extent of privacy interests implicated in a cell phone search is necessary for this Court to consider when "balancing [a search's] intrusion on the individual's Fourth Amendment interests against [the search's] promotion of legitimate governmental interests" in the border search context. *Montoya de Hernandez*, 473 U.S. at 537 (internal quotation marks omitted). As explained in *Sultanov*, Supreme Court and Second Circuit precedent make it clear that a traveler's Fourth Amendment interest in a personal cell phone is extremely high. *See Sultanov*, 742 F. Supp. 3d at 279–88.

To properly consider the "governmental interest" side of the equation in this context, the Court looks to the history behind the border search exception. The border search exception is primarily derived from "the government's legitimate interest in protecting the integrity of the border by preventing 'illegal articles' (including goods subject to duty) and inadmissible foreign citizens from entering the country." *Id.* at 285 (collecting cases) (finding that "[s]earching and seizing the data on a person's phone does not prevent that data . . . from entering and circulating within the country"). While there is of course always a general governmental interest in detecting and seizing contraband, especially CSAM, the extent to which that interest aligns with the justification for the border search exception is far from clear "when

the government searches data stored on a person's cell phone." *Id.* Thus, "[g]iven the extraordinary intrusion into a person's privacy posed by a cell phone search, this Court has no difficulty concluding that a manual search of a cell phone at the border is a nonroutine search to which a categorical border search exception does not apply." *Id.* at 288.[3]

After finding that the search of a cell phone is "nonroutine," a Court must then decide the requisite degree of suspicion required for the search to be reasonable under the Fourth Amendment. In *Sultanov*, this Court noted that the other circuit courts, and most district courts within the Second Circuit, which have recognized that law enforcement must have some degree of individualized suspicion to search a cell phone at the border, have not gone so far as to require a warrant. *See id.* at 290 (collecting cases). However, taking into consideration the various factors that bear on the Fourth Amendment's touchstone of "reasonableness" — including a person's heightened privacy interest in the vast contents of her cell phone, the remarkable speed at which a warrant can be obtained in modern times, the interest in preventing the flow of contraband that grounds the border-search exception, and the profound First Amendment concerns implicated by border agents conducting warrantless searches of travelers' cell phones and gaining "intimate window[s]" into virtually every aspect of their personal and professional lives — this Court concludes that the

[3] This Court in *Sultanov* also found that because both manual and forensic searches of cell phones "involve[d] . . . a vast intrusion on a traveler's privacy," "the privacy intrusion of a manual search is substantially the same, for Fourth Amendment purposes, as the privacy invasion of a forensic search." *Id.*

government must have a warrant and probable cause to search a cell phone at the border. *See id.* at 296 (quoting *Carpenter v. United States*, 585 U.S. 296, 311 (2018)).

Although this Court recognizes that the Second Circuit may well resolve this issue in the near future, at this writing, the government has presented no intervening case law or novel arguments that lead the Court to revisit its holding in *Sultanov*. Therefore, this Court concludes that the warrantless search of Robinson's iPhone on November 14, 2022, was conducted in violation of his Fourth Amendment rights. Accordingly, the contents revealed in that search, as well as all "evidence obtained from or as a consequence" of the search, is subject to exclusion. *Costello v. United States*, 365 U.S. 265, 280 (1961) (internal quotation marks omitted).

Accordingly, the evidence obtained "as a direct result of [the] illegal search or seizure" as well as evidence that is "derivative of [the] illegality" is subject to suppression. *United States v. Cacace*, 796 F.3d 176, 188 (2d Cir. 2015) (quoting *Segura v. United States*, 468 U.S. 796, 804 (1984)). As the warrantless search by Officer Nunes at JFK was a "[b]ut-for" cause of the subsequent search by HSI agent Anstee, and unquestionably provided the probable cause for a forensic search of Robinson's phone cited in the search warrant affidavit by Agent Stepien, all the fruits of the initial search of Robinson's iPhone are subject to suppression as well. *See Hudson v. Michigan*, 547 U.S. 586, 592 (2006).

## II. The Good Faith Exception

The Court next turns to the government's claim that, even if probable cause and a warrant were necessary to search Robinson's phone at the border, evidence

from his phone should not be suppressed as it was obtained in good faith by law enforcement. *See* Gov't Opp. 23–27 (citing *United States v. Leon*, 468 U.S. 897, 908 (1984) ("[W]hen law enforcement officers have acted in objective good faith or their transgressions have been minor, the magnitude of the benefit conferred on such guilty defendants offends basic concepts of the criminal justice system.").

**A. Legal Standards and Summary of Findings**

The government makes two core arguments as to why the good faith exception to the exclusionary rule should apply here. The first involves the initial search at JFK Airport. The government argues that Officer Nunes had a reasonable belief that the manual search of the cell phone at JFK airport was "routine" and thus required no individualized suspicion; alternatively, if it was "nonroutine," she had "reasonable suspicion" to search the phone, and therefore had a good faith basis to believe that her actions did not violate Robinson's Fourth Amendment rights. *Id.* at 24–25. The government's second argument is that the issuance of the warrant itself provides the requisite good faith: that is, that the subsequent forensic search was authorized by a judicial warrant, and HSI reasonably relied on that warrant when the agency conducted its forensic search of the iPhone. *See id.* at 25–27.

The Supreme Court has recognized two applications of the good faith exception to the exclusionary rule that may apply here. The first is when a search is conducted in "objectively reasonable reliance on binding appellate precedent," *Davis v. United States*, 564 U.S. 229, 249–50 (2011). The second is when a search is conducted in "objectively reasonable reliance on a subsequently invalidated search warrant."

*Leon*, 468 U.S. at 922; *but see id.* at 923 (suppression "remains an appropriate remedy" where, *inter alia*, a court finds that the magistrate judge who issued the warrant "was misled by information in an affidavit that the affiant knew was false" or where the affiant exhibited a "reckless disregard of the truth").

If neither of those two circumstances apply, that does not end the inquiry. For even if officers in the field who conduct a warrantless search or seizure lacked a good faith basis to believe their actions were constitutional, evidence will still only be excluded when the "corrective value [of exclusion] justifies its cost." *United States v. Raymonda*, 780 F.3d 105, 117–18 (2d Cir. 2015). This cost is justified when "the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Id.* at 118 (internal quotation marks omitted). On the other hand, "when police act with an *objectively* reasonable good faith belief that their conduct is lawful, or when their conduct involves only simple, isolated [instances of] negligence," exclusion is inappropriate. *Id.* (internal quotation marks omitted) (emphasis supplied). This is because the remedy of suppression is not borne out of any explicit text from the Fourth Amendment. Rather, the "Supreme Court has established an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial." *United States v. Lauria*, 70 F.4th 106, 121 (2d Cir. 2023) (alterations adopted and internal quotation marks omitted). The rule was created not as a "means to 'redress the injury' of an unconstitutional search" but rather was "designed to deter future Fourth Amendment violations." *Raymonda*, 780 F.3d at 117 (quoting *Davis*, 564 U.S. at 236); *see also Herring v. United States*, 555 U.S. 135,

141 (2009) ("[T]he exclusionary rule is not an individual right and applies only where it results in appreciable deterrence." (alterations adopted and internal quotation marks omitted)). Because deterrence is the goal of the exclusionary rule, for it to apply, "police conduct must be sufficiently deliberate that exclusion can meaningfully deter it." *Herring*, 555 U.S. at 144.

For the reasons that follow, the Court finds that the government cannot rely upon either of its proposed good faith exceptions to the exclusionary rule. First, with regard to the manual search by border agents, there was no binding precedent that authorized a so-called "routine" search of Robinson's iPhone on which a reasonable officer could have relied. And even if the agents had a good faith basis to believe that no judicial warrant was required and they needed only reasonable suspicion, the staleness and limited information in the TECS Report that provided the sole ground for the search did not permit them to conduct the search under then-existing appellate caselaw that governs certain "nonroutine" searches at the border. And after weighing the societal cost of exclusion against its "corrective value," *Raymonda*, 780 F.3d at 117–18, the Court finds that suppression is warranted.

Second, the government has not shown that the subsequent forensic search of Robinson's phone was conducted in a good faith reliance on the warrant. This is because, as explained below, the magistrate judge was not provided with critical facts surrounding the government's earlier seizure of the evidence that supported the probable cause determination. Instead, the record demonstrates that Agent Stepien (1) presented the magistrate judge with an incomplete and misleading affidavit in

support of the warrant, which falsely implied that the search of Robinson's phone at JFK was a routine, suspicionless "border search," and deliberately omitted the fact that it was actually conducted pursuant to a three-year-old TECS report; and (2) falsely suggested that the search was performed after Robinson gave his "voluntar[y]" consent, when that was not the case; for even the government does not contend that this case falls within the Fourth Amendment's consent exception, since Robinson was directed, not asked, to surrender his phone and provide his passcode at the time he was individually targeted for an electronic media search.

**B. The Manual Search of Robinson's iPhone on November 14, 2022**

The government first argues that even if the Court were to conclude that the manual search conducted on Robinson's cell phone on November 14, 2022, was unconstitutional, CBP Officer Nunes searched the iPhone "with an objectively reasonable good-faith belief that [her] conduct [was] lawful." Gov't Opp. at 24 (quoting *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018) (quoting *Davis*, 564 U.S. at 238). The Court disagrees. After hearing her in-court testimony, the Court has no doubt that Officer Nunes *subjectively* believed that her actions were in accordance with (indeed, required by) CBP policy and the directives of her supervisors as she understood them. But that is not the issue here. Ultimately, the good faith exception does not apply because the government has not shown that there was an *objective* basis — supported by binding appellate caselaw — upon which Officer Nunes could have reasonably relied to believe that this particular search was constitutional.

It is well settled that searches "conducted in objectively reasonable reliance on binding precedent are not subject to the exclusionary rule." *Davis*, 564 U.S. at 232. The Second Circuit has held that "binding precedent refers to the precedent of this Circuit and the Supreme Court." *United States v. Aguiar*, 737 F.3d 251, 261 (2d Cir. 2013) (internal quotation marks omitted). Therefore, if Officer Nunes reasonably believed that "binding precedent" of this Circuit or the Supreme Court authorized the search, the fruits of the search would not be subject to suppression. The government has failed to make that showing here.

*i. Binding Appellate Precedent Would Not Lead a Reasonable Officer to Believe that the Search of an iPhone Was "Routine"*

The government first argues that Officer Nunes reasonably relied on binding appellate precedent in believing that the search was "routine," and therefore did not require any modicum of suspicion. *See* Gov't Opp. at 24 ("[A] reasonable officer or agent could believe that the search in question was routine . . . ."). The government contends that because there was no binding precedent *precluding* suspicionless searches of cell phones at the border, Officer Nunes "rel[ied] in good faith on the existing state of the law" in searching Robinson's iPhone. Gov't 12/27/2024 Ltr. at 3.

The first flaw in this argument is its initial premise: it reverses the burden the good faith exception places on law enforcement. The good faith exception does not permit the law enforcement to engage in any and all warrantless searches until an appeals court forbids it. Rather, there must be actual "binding precedent" on which a reasonable officer could rely in believing that the search was lawful — *i.e.,* that it fell within an established exception to the Fourth Amendment's warrant

requirement. *Davis*, 564 U.S. at 241; *see also United States v. Fox*, No. 23-cr-225 (NGG), 2024 WL 3520767, at *18 n.34 (E.D.N.Y. July 24, 2024) (noting that, unlike qualified immunity, "exclusion does not require a violation of 'clearly established law'" (quoting *Mullenix v. Luna*, 577 U.S. 7, 11 (2015)).

At the time of the search of Robinson's iPhone, "neither the Supreme Court nor the Second Circuit ha[d] addressed the lawfulness of warrantless searches of cell phones at the border." *Alisigwe*, 2023 WL 8275923, at *7. However, the Second Circuit had long recognized that not all searches at the border were alike. Specifically, the Circuit had long held that border searches considered to be "non-routine" required at least reasonable suspicion to be constitutional. *See Irving*, 452 F.3d at 124.

The first question, then, is whether a reasonable officer could have objectively believed, in November 2022, that there was "binding appellate precedent" within this Circuit holding that a search of an international traveler's iPhone was a "routine" search requiring no individualized suspicion. On this issue, *Irving* provides a useful anchor point. *Irving* involved the warrantless border search of computer diskettes in a passenger's luggage — a rudimentary form of electronic media storage that is vastly different in kind than what is contained on modern smart phones.[4] The *Irving* court

[4] The search in *Irving* concerned a "disposable camera and two 3.5 inch computer diskettes," commonly known as floppy disks. *Irving*, 452 F.3d at 115. Floppy disks "featured 1.44 megabytes of storage space." *Floppy Disk Storage*, IBM, https://www.ibm.com/history/floppy-disk (last visited May 4, 2025). For comparison, Robinson's iPhone that was searched was an "Apple iPhone XS," Warrant Aff. ¶ 4, of which the base model has a storage capacity of 64 gigabytes, *iPhone XS – Technical Specifications*, Apple, https://support.apple.com/en-us/111881 (last visited May 4,

analyzed the search under the higher standard of a "nonroutine" border search, asking whether the agents had reasonable suspicion. Because the court was satisfied that reasonable suspicion justified the search in Irving's case, it did not reach the issue of whether this kind of search should, in general, be considered "routine" or "non-routine." *Id.* Thus, in 2006 — more than a decade before the Supreme Court provided the guidance in *Riley* that the search of a cell phone "differ[ed] in both a quantitative and qualitative sense" from the search of other objects, *Riley*, 573 U.S. at 393 — the Second Circuit acknowledged that the search of a far less substantial cache of electronic data at the border may not be a "routine" search.

More fundamentally, the government has pointed this Court to *no* Second Circuit or Supreme Court precedent holding — or even suggesting — that law enforcement's search of a modern cell phone and the breathtaking amount of personal information it holds could ever be considered a "routine" border search. Nor has it cited any case in which the Second Circuit or the Supreme Court found "routine" a search in which the level of intrusion was in any way analogous to the search of a traveler's iPhone.

It is true that in *United States v. Levy*, the Second Circuit, in a footnote that might reasonably be construed as dicta, noted that "we have suggested that the label 'non-routine' should *generally* be reserved for intrusive border searches of the person (such as body-cavity searches or strip searches), not belongings." 803 F.3d 120, 123

---

2025). As there are 1,000 megabytes in a gigabyte, Robinson's iPhone had at least approximately 44,444 times more storage than one of Irving's floppy disks.

n.3 (2d Cir. 2015) (emphasis supplied). *Levy* did not involve any sort of electronic evidence; the Court was asked to decide only whether border officials had lawfully searched and copied a traveler's notebook. *See id.* at 123. Notably, however, when addressing whether the search of a simple notebook was "routine" or "non-routine," the *Levy* Court "avoid[ed] resolving that question" and simply held that suppression was unwarranted because law enforcement had reasonable suspicion to conduct the search in Levy's case. *Id.*

Thus, even construing the caselaw in the light most favorable to the government, Second Circuit precedent as to whether the search of a cell phone at the border was routine or nonroutine in November of 2022 was, at the very most, unsettled. And unsettled law is not "binding appellate precedent" upon which law enforcement can reasonably rely to justify a suspicionless search. *Davis*, 564 U.S. at 241.

Indeed, all binding appellate precedent in 2022 strongly supported the opposite conclusion: that the search of an electronic device is nonroutine because it is clearly of a difference in kind than the search of a person's other belongings (like, for example, a notebook). In 2016, for example, the Second Circuit, sitting *en banc*, held that the level of intrusion caused by the search of a computer hard drive is not analogous to that caused by the search of an entire file cabinet, as "no file cabinet has the capacity to contain as much information as the typical computer hard drive." *Ganias*, 824 F.3d at 217; *see also Riley*, 573 U.S. at 393–94 (finding that the search of a cell phone was unusually invasive because it could permit the government to

reconstruct "[t]he sum of an individual's private life . . . through a thousand photographs labeled with dates, locations, and description").

It is important to note that all an officer may rely on in good faith is binding appellate precedent. The government presented evidence that it was CBP policy that the phone of any passenger may be subject to search upon entry into the country. *See* Hr'g Tr. at 54 (Officer Nunes explaining that a "tear sheet" is given to a passenger whose phone is searched that "explains CBP's authority to search electronic devices"); Tear Sheet at 3 (informing passengers that "[a]ll persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention" and that the passenger is "receiving this sheet because [their] electronic device(s) have been detained for further examination"). Officer Nunes also confirmed that in this case she had no "discretion not to conduct the electronic exam" of Robinson's iPhone. Hr'g Tr. at 78. But CBP policy and practice does not determine whether an officer relied on binding appellate caselaw. The line between a routine and nonroutine search is not determined by "how ordinary or commonplace [the] search is, but rather the level of intrusion into a person's privacy." *Tabaa v. Chertoff*, 509 F.3d 89, 98 (2d Cir. 2017) (internal quotation marks omitted). CBP's apparently widespread policy of performing manual searches of cell phones at the border and informing travelers that it had the broad authority to do so simply does not bear on whether the agents' actions in Robinson's case were authorized by binding appellate precedent.

Not only was there was no binding appellate precedent in November 2022

holding that border searches of cell phones are "routine" searches that may be conducted in the absence of reasonable suspicion, but also, relevant precedent strongly indicated that the search of a cell phone was a significant "level of intrusion into a person's privacy," *id.* (quoting *Irving*, 452 F.3d at 123), and therefore nonroutine. Thus, no reasonable officer could have relied on binding precedent to believe that the search of Robinson's iPhone at the border was routine and could be conducted "even without reasonable suspicion." *Levy*, 803 F.3d at 122 (internal quotation marks omitted).

*ii. The Search of Robinson's Cell Phone was Not Supported by Reasonable Suspicion*

Given that the Officer Nunes could not have reasonably relied on the "routine" border search exception to conduct a suspicionless search of Robinson's iPhone, the Court next considers if the facts known to her at the time provided a good faith basis to conclude that a "nonroutine" border search was justified. While this Court, as explained *supra*, concludes that the Fourth Amendment requires probable cause and a warrant to conduct a manual search of a cell phone at the border, it recognizes that neither the Supreme Court nor the Second Circuit had yet decided this issue at the time Robinson's phone was searched in November 2022. (Nor has either court done so as of the date of this opinion.) Additionally, the highest degree of suspicion that the Second Circuit has found necessary in a nonroutine search is "reasonable suspicion." *See, e.g., Levy*, 803 F.3d at 124; *Irving*, 452 F.3d at 124; *United States v. Ogberaha*, 771 F.2d 655, 657 (2d Cir. 1985). Thus, if the objective facts available to Officer Nunes created a reasonable suspicion that there was contraband on

Robinson's iPhone at the time he presented himself at CBP, the government would have a stronger argument that the initial manual search was "conducted in objectively reasonable reliance on binding appellate precedent." *Davis*, 564 U.S. at 231. On this record, however, the government fails to make even that showing.

An officer's reasonable suspicion must be supported by "specific and articulable facts" that, "taken together with rational inferences," provide that officer with an objective basis for a search. *United States v. Compton*, 830 F.3d 55, 61 (2d Cir. 2016) (internal quotation marks omitted). In the context of a border search, "reasonableness is defined by weighing the warranted suspicion of the border official against the offensiveness of the intrusion." *Asbury*, 586 F.2d at 976. The Second Circuit has "pointed to a number of factors that courts may consider in making the reasonable suspicion determination, including unusual conduct of the defendant, discovery of incriminating matter during routine searches, computerized information showing propensity to commit relevant crimes, or a suspicious itinerary." *Irving*, 452 F.3d at 124. Because this Court has already held that the "offensiveness of the intrusion" of a cell phone search is high, it must measure the "warranted suspicion of the border official." *Asbury*, 586 F.2d at 976.

The government argues that the TECS report regarding Robinson, standing alone, provided Agent Nunes with reasonable suspicion that he possessed CSAM on his phone. *See* Gov't Opp. at 23. The TECS report was generated three years before Robinson's phone was searched, on November 11, 2019. TECS Report at 1; *see* Hr'g Tr. at 50. The full contents of the alert, as presented to Officer Nunes, read: "Subj

linked to the purchase of child sexual exploitation material via FinCen. Refer to Secondary for interview & media device exam to include cell phones and laptops."[5] TECS Report at 2.

Nunes confirmed that the entry on Robinson was a "prime hit" — meaning that the "system ha[d] determined that the person that's in front of the officer is 100 percent the person in the record." Hr'g Tr. at 98–99. However, a "prime hit" does not indicate anything about the reasons why the TECS Report was created; it merely confirms that the traveler is the person whom the alert was intended to flag for inspection.

Once a CBP officer at JFK Airport is alerted to a prime hit, it "requires a mandatory referral to secondary for inspection." *Id.* Officer Nunes also testified that the TECS hit was generated by a division of CBP called the National Targeting Center ("NTC"). *See id.* at 101. In the case of a prime hit lookout generated by the NTC, there is typically no discretion as to whether or not the officer conducts an electronic media exam. Hr'g Tr. at 103–04. Nunes indicated that she may have discretion only when it is clear that the "hit ha[d] been resolved," such as when the

[5] Officer Nunes testified that she "vaguely remember[ed] that [she] [thought] there was an update" to the TECS lookout, which was "maybe a year prior" to the encounter but she was "not a hundred percent sure." Hr'g Tr. at 51. At the hearing, she also reviewed each page of the lookout and confirmed that there was nothing on those pages indicating that the report had been "refreshed" or "updated" approximately one year after it was entered. *Id.* at 87–88. Based on the Court's assessment of Officer Nunes' in-court testimony, and the fact that she was candid about the fact that this was a "vague[]" recollection, the Court finds, for purposes of this motion, that the TECS lookout was entered in November 2019, and that there is no evidence that it was updated at any time before Robinson landed at JFK in November 2022.

system indicates that another officer already "fully addressed whatever the lookout was." *Id.* Nunes also testified, however, that prime-hit lookouts "don't expire." *Id.* at 104. And even if Nunes interviews a traveler who is subject to a TECS lookout, and releases the traveler after she has determined that the reason for the detention has been "fully addressed," an NTC-generated lookout will remain in the system until someone at "a different division" of CBP removes it. *Id.* at 104–05. Nunes herself has no ability to remove an NTC lookout from TECS, even when it has been "closed out" by her. *Id.*

The government also called Agent Egbert Simon, formerly a Supervisory Customs and Border Protection Officer and now a Special Agent with the United States Attorney's Office. *Id.* at 107–08. Agent Simon played no role in the investigation of Robinson, *id.* at 110, and had never been detailed at NTC, *id.* at 119, but testified to his understanding of how TECS reports are generated by the National Targeting Center and how they are viewed by officers at the border. He described the NTC as "like an intelligence hub for frontline personnel." *Id.* at 113. In his view, when a lookout is generated by the NTC, "you're going to feel that they have already done their . . . research and their analysis for creating that record." *Id.*; *see also id.* at 114 ("[I]f it's from NTC, we're going off the basis that there's some type of research or intel behind it."). Agent Simon also confirmed that while lookouts issued by CBP officers in the field only remain valid for one year, that expiration date does *not* apply to lookouts generated by anyone at NTC. *Id.* at 117, 126. Thus, a single lookout generated by an agent at the National Targeting Center could remain in TECS

indefinitely. *Id.*

It is true, as the government argues, that "a TECS hit can significantly factor into a reasonable suspicion finding." Gov't Opp. at 22. But here, the TECS hit did not just "factor significantly" into CBP's decision to search Robinson's cell phone. It is the *only* evidence the government cites in support of its claim that Officer Nunes had a reasonable suspicion that Robinson was in possession of CSAM on his iPhone on November 14, 2022. *See id.* at 21–23. Yet the government has cited no case, from any jurisdiction, in which any court has held that a TECS hit with this paucity of information, standing alone, established the requisite reasonable suspicion to conduct a nonroutine border search. And it certainly has not pointed this Court to any case in which a three-year-old TECS hit provided the requisite reasonable suspicion.

Instead, every case the government relies upon in which reasonable suspicion existed involves a TECS hit combined with other factors. In the Ninth Circuit case of *United States v. Cotterman*, for example, a TECS hit indicated not only that the defendant was a registered sex offender whose prior convictions involved multiple acts of sexual abuse against children, but also that he was "potentially involved in child sex tourism." 709 F.3d at 957, 969. As the court noted, CBP was alerted to the fact that Cotterman frequently traveled outside the United States and was returning from a "country associated with sex tourism," and the agent was specifically informed by Immigration and Customs Enforcement that the TECS alert had been generated by Operation Angel Watch, a specialized law enforcement unit that "targeted

individuals potentially involved in sex tourism." *Id.* at 968–69. The Court concluded that "[defendant's] TECS alert, prior child-related conviction, frequent travels, crossing from a country known for sex tourism, and collection of electronic equipment, plus the parameters of Operation Angel Watch program, taken collectively, gave rise to reasonable suspicion." *Id.* at 969.

Similarly, in *United States v. Whitted*, while the government did rely on a TECS hit which indicated a "one-day lookout" for the defendant in establishing reasonable suspicion, the law enforcement officer "conducted further inquiries in the TECS and discovered that [defendant's] ticket has been purchased at the last minute," that he "traveled to other drug source countries" and that he had a "criminal record." 541 F.3d 480, 483 (3d Cir. 2008). The Third Circuit found that these were "numerous facts" which "raised the suspicion that that Whitted was involved in drug smuggling." *Id.* at 490. Nor is this case analogous to *Irving*, in which the Second Circuit found that there was reasonable suspicion to search the defendant's computer diskettes. Gov't Opp. at 23. In *Irving*, the Second Circuit based its reasonable suspicion determination not only on the fact that the defendant "was the subject of a criminal investigation," but also that he "was a convicted pedophile," that he "had been to Mexico," that "he claimed that he visited an orphanage while in Mexico," and that "his luggage contained children's books and drawing that appeared to be drawn by children." 452 F.3d at 124.[6]

[6] In addition to the Circuit Court decisions cited above, the government also cites *United States v. Ramirez*, in which a district court in the Western District of Texas found that border agents had reasonable suspicion to search the phone of a

Here, by contrast, the only information provided to Officer Nunes was a three-year old electronic notification that the person in front of her was "linked to the purchase" of CSAM. TECS Report at 2. It is undisputed that "customs officers should be able to rely on data provided by computer reports to create reasonable suspicion for a search." *Whitted*, 541 F.3d at 490. However, the information relied upon must itself create the requisite suspicion. Even taking into account the facts that this was a "prime hit" (which confirmed that Robinson was the person to whom the November 2019 entry referred) and generated by the National Targeting Center, all that demonstrates is that a unit of CBP — which acts as its "intelligence hub for field personnel," Hr'g Tr. at 119 — possessed information about a possible "link[]" to a CSAM purchase by Robinson from three years earlier, TECS Report at 2. And for several reasons, that alone was insufficient to provide a reasonable suspicion that Robinson possessed CSAM on his phone on November 14, 2022.

First, Officer Nunes did not know if the TECS hit from November 11, 2019, was in reference to a single isolated purchase, or multiple purchases over a longer

---

defendant who was diverted to secondary inspection based on a TECS hit that (as here) linked him to the possible purchase of child pornography. No. EP-18-cr-3530 (PRM), 2019 WL 3502913, at *1 (W.D. Tex. Aug. 1, 2019). But that case is inapposite, since in *Ramirez,* the court made a factual finding (after an evidentiary hearing) that the defendant immediately gave his knowing and voluntary consent to search his device, and *during that consent search*, child pornography was lawfully discovered and seized. *Id.* at *6–12. Here, by contrast, the government is not contending that Robinson consented to the search of his phone, but rather that CBP had the legal authority to compel him to submit to a device search because the TECS hit alone provided the requisite reasonable suspicion. *See* Oral Arg. Tr. at 69 (confirming that the government is not contending that either CBP or HSI searched Robinson's phone on consent).

period of time. And while certainly giving rise to a potentially important investigative lead at the time the hit is generated, even if the information were accurate, a single purchase of contraband does not necessarily create a reasonable suspicion that the person is in possession of such contraband three years later. Additionally, even though it was a prime hit, the TECS report does not even affirmatively state that Robinson "purchased" CSAM, but rather that he was "linked to the purchase" of CSAM. TECS Report at 2. A person could be "linked to the purchase" of contraband without purchasing the contraband themselves — for example, if a credit card was used without their knowledge by another member of their household. Or a person could be the victim of credit card fraud and unaware of the fact that their stolen card was used to purchase digital contraband. The Court notes that this is not a *de minimis* risk in the modern era: according to the Federal Trade Commission, in 2020 alone, there were 1,387,615 reports of identity theft in the United States. *See* Office of the New York State Comptroller, *The Increasing Threat of Identity Theft* 3 Fig. 1 (May 2021), https://www.osc.ny.gov/files/reports/pdf/increasing-threat-of-identity-theft.pdf.

This is not to say that a single TECS hit linking someone to an earlier purchase of contraband, including but not limited to CSAM, could never provide reasonable suspicion that the person possessed contraband at the border. The government's case for reasonable suspicion would be much stronger, if, for instance, the information available to the border agent was that Robinson had been linked to a purchase of CSAM in the week he was traveling abroad, especially if that purchase was connected

to an IP address in the country from which he was arriving. That was decidedly not the case in this instance. And as noted above, the government has found no case — and this Court knows of none — in which a TECS hit linking the subject to the purchase of CSAM, and nothing else, provided reasonable suspicion to conduct a warrantless search of a traveler's devices.

The age of the TECS report itself also cuts strongly against a finding of reasonable suspicion here. As the Second Circuit has long recognized, even reliable information that would otherwise provide grounds for a search can go stale. "[T]he principal factors in assessing whether or not the supporting facts have become stale are the age of those facts and the nature of the conduct alleged to have violated the law." *Diamondstone v. Macaluso*, 148 F.3d 113, 124 (2d Cir. 1998) (internal quotation marks omitted). While the Circuit has primarily addressed the issue of staleness in the context of probable cause, "courts in this Circuit have generally found that the information necessary to support a finding of probable cause should be no older than a year." *United States v. Bazemore*, No. 20-cr-573 (ER), 2021 WL 1719233, at *4 (S.D.N.Y. Apr. 30, 2021) (internal quotation marks omitted) (collecting cases); *cf. United States v. Gallo*, 863 F.2d 185, 192 (2d Cir. 1988) (noting that where the conduct is continuing, "the passage of time" becomes less significant). That probable cause benchmark provides important guidance in assessing whether a single piece of information about a traveler's purchase(s) within the United States can provide reasonable suspicion that he possesses contraband at the border three years later.

Of course, deciding whether an investigative lead into the possible purchase of

child pornography is stale requires a court to consider the nature of the contraband itself. On this point, the Court credits the testimony of Agent Stepien that, in a substantial number of cases he has investigated or otherwise learned about, the collection of child pornography "doesn't just stop with one download. It's usually over years of collection until either they get caught[,] or, you know, something else happens." Hr'g Tr. at 131–32. However, this does not mean that information related to a suspected purchase of child pornography *never* goes stale — as the Second Circuit has expressly recognized. In *Raymonda*, the Second Circuit acknowledged that hoarding of images is common among those involved in the trade of child pornography. *See* 780 F.3d at 115. Nevertheless, the Court found that "nine-month-old evidence" that a user with an IP address associated with the defendant's home opened pages that had thumbnail links housing child pornography did "not create a fair probability that child pornography [would] still be found on [defendant's] computer" months later. *Id.* at 116–17. The *Raymonda* court distinguished that case from those in other Circuits where past information regarding the suspect's interaction with digital CSAM was not stale: for example, where the suspect not only downloaded images but uploaded them as well, or where a suspect was shown to have had to "enter a decoded URL address and decrypt" a download, or where a suspect had registrations to websites and did not cancel his memberships. *See id.* at 114–15 (collecting cases). Those are all circumstances, the Court explained, which "tend[ed] to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter" and suggested — "as is common among persons

interested in child pornography — [the suspect] likely hoarded the images he found." *Id.* at 115.

As in *Raymonda*, the three-year-old TECS report in the instant case had nothing in it to suggest that Robinson's "brush with child pornography was [not] a purely negligent or inadvertent encounter." *Id.* Of course, the photographs and videos seized from Robinson's devices in November 2022 now strongly indicate otherwise. But reasonable suspicion is based on what was known to the officer at the time of the search. And here, Officer Nunes had no information about Robinson except for that single, three-year-old TECS hit — no criminal record, no continuing downloads, no incriminating statements, no suspicious travel history to locations known for child sexual exploitation. Thus, even assuming, *arguendo,* that the government had reasonable suspicion in 2019 that Robinson had purchased CSAM, that does not make a search of his phone upon returning from a one-time vacation abroad with his spouse three years later "reasonably related in scope to the circumstances which justified it initially." *Montoya de Hernandez*, 473 U.S. at 542.

*iii. Cost of Suppression Balanced Against Deterrence Value*

In determining whether suppression is appropriate, this Court must conduct "the cost/benefit analysis required by *Herring,*" which permits the Court to exclude evidence only if "the costs of letting a guilty defendant go free" are outweighed by the "benefits of deterrence." *Julius*, 610 F.3d at 67–68 (quoting *Herring*, 555 U.S. at 141); *see also Pa. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 368 (1998) ("We have never suggested that the exclusionary rule must apply in every circumstance in which it

might provide marginal deterrence."). Because the exclusionary rule is a means of deterring unconstitutional law enforcement conduct, "it is applicable only where its deterrence benefits outweigh its substantial social costs." *Scott*, 524 U.S. at 363 (internal quotation marks omitted). The Supreme Court has acknowledged that the exclusion of evidence comes with "substantial social costs," as "[i]t almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence." *Davis*, 564 U.S. at 237 (internal quotation marks omitted). "Nevertheless, society must swallow this bitter pill when necessary; specifically, when the deterrence benefits of suppression . . . outweigh its heavy costs." *Lauria*, 79 F.4th at 121 (alteration in original and internal quotation marks omitted).

As a starting point, the exclusion of inculpatory evidence always comes at a cost to "truth and the public safety." *Davis*, 564 U.S. at 232. As the Supreme Court has stated, "letting guilty and possibly dangerous defendants go free . . . offends basic concepts of the criminal justice system." *Herring*, 555 U.S. at 141 (internal quotation marks omitted).

Those concerns are further heightened where, as here, a defendant is charged with an offense involving child pornography. That is true even though the instant case involves the possession of CSAM, rather than its production or sale, and even though Robinson has not been accused of any unlawful sexual contact with a minor. This is not to say that all CSAM-related charges are equivalent in terms of the harm they cause. As the Sentencing Commission has noted, "not all child pornography offenders are pedophiles, and not all child pornography offenders engage in other sex

offending." U.S. Sentencing Comm'n, *Federal Child Pornography Offenses* (Dec. 2012), at 73; *see also United States v. R.V.*, 157 F. Supp. 3d 207, 239 (E.D.N.Y. 2016) (JBW) (citing to research finding that "for most offenders, their online offending has no behavioural link to contact sex offending" (alteration adopted) (quoting Hana Lena Merdian *et al.*, *The Three Dimensions of Online Child Pornography Offending*, 19 J. of Sexual Aggression 121, 123 (2013)).

Yet even the non-producing consumers of child pornography perpetrate extreme harm upon children. A child is victimized not only when the abuse that is depicted in CSAM first takes place; "[t]hey are further victimized each time that record is accessed." Richard Wortley & Stephen Smallbone, U.S. Dep't of Justice, Off. of Community Oriented Policing Servs., *Child Pornography on the Internet*, Problem-Oriented Guides for Police Problem-Specific Guides Series No. 41, at 15 (May 2006), https://popcenter.asu.edu/sites/default/files/child_pornography_on_the_internet.pdf. As reported by victims, this is because often "th[e] initial feelings of shame and anxiety did not fade but intensified to feelings of deep despair, worthlessness, and hopelessness." *Id.* Indeed, in the same report in which the Sentencing Commission recognized that consuming child pornography is different than other sex offenses, it also emphasized that "[c]hild pornography offenses *inherently involve* the sexual abuse and exploitation of children. Victims are harmed initially during the production of child pornography, but the perpetual nature of the distribution of images on the Internet causes a significant, *separate*, and continuing harm to victims." U.S. Sentencing Comm'n, *Federal Child Pornography Offenses*, at 311

(emphasis supplied). The consumption and possession of child pornography is far from a victimless crime. "When the pornographic images are viewed by others, the children depicted are victimized once again." Audrey Rogers, *Child Pornography's Forgotten Victims*, 28 Pace L. Rev. 847, 853 (2008). Thus, this Court recognizes the strong government interest in rooting out and removing CSAM from circulation, a goal achieved in part by its ability to bring criminal prosecutions that hold purchasers accountable and deter others from making such purchases.

On the other side of the equation, the Court must weigh the value of deterrence. To warrant exclusion, "[p]olice conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *United States v. Jones*, 43 F.4th 94, 110–11 (2d Cir. 2022) (internal quotation marks omitted). In assessing culpability, the Court can consider whether the law enforcement action was "a deliberate strategic choice" to evade the general warrant requirement. *United States v. Stokes*, 733 F.3d 438, 444 (2d Cir. 2013).

Importantly, "[t]he pertinent analysis of deterrence and capability is objective, not an inquiry into the subjective awareness" of the officer performing the search. *Herring*, 555 U.S. at 145 (internal quotation marks omitted). Thus, the inquiry does not turn on whether Officer Nunes was aware that she violated the Fourth Amendment when she searched Robinson's phone, but whether "a reasonably well trained officer would have known that the search was illegal." *Leon*, 468 U.S. at 922 n.23. As discussed *supra*, this Court finds that no reasonably well-trained officer

could have believed that binding appellate precedent authorized the search of Robinson's phone. Instead, CPB instituted, and required Officer Nunes to follow, a policy of *mandatory* electronic-device searches at JFK airport based on a single TECS hit from a different division of CBP that could have been (and was) entered years earlier — no matter the traveler's personal history, itinerary, potential explanations for the TECS hit, or conduct at the airport. *See, e.g.,* Hr'g Tr. at 78 (in light of the TECS prime hit from NTC, Nunes "did not have a choice" as to whether or not to search Robinson's phone).

Testimony at the suppression hearing also revealed that a TECS hit entered by an agent at the NTC may remain in the system indefinitely. *See* Hr'g Tr. at 117, 126. At oral argument, the government took the position that any TECS hit such as this one, no matter how long it had been in the system, would give CBP agents the necessary reasonable suspicion to conduct a search of that traveler's cell phone, as long as the alert had not been "resolved." *See* Oral Arg. Tr. at 70–72. This Court disagrees. It simply cannot be the case that an agent at the so-called "National Targeting Center" can — in entering a single "lookout" targeting a person for the suspected purchase of contraband — create the requisite reasonable suspicion that might allow the person's electronic devices to be searched upon reentry into the country for the rest of her life.

The official policies that led to this search were thus, at the very least "grossly negligent." *Herring*, 555 U.S. at 144. And as the Supreme Court recognized in *Herring,* deterrence may be well served "[i]n a case where systemic errors were

demonstrated." *Id.* at 146; *see also Hudson*, 547 U.S. at 604 (Kennedy, J., concurring in part and concurring in judgment) ("If a widespread pattern of violations were shown . . . there would be reason for grave concern."). This Court is indeed "gravely concern[ed]" about what appears to be a mandatory electronic-device-search policy for a sweeping category of TECS hits, of any age, even a decade after the Supreme Court made clear in *Riley* that a search of a person's cell phone represents such a vast intrusion on personal privacy that it warrants particularly demanding Fourth Amendment scrutiny. The present record also shows the absence of any controls at JFK Airport to ensure that CBP searches the electronic devices of only those travelers for whom the agency possesses particularized, non-stale evidence that may be in possession of contraband on those devices at the time they reenter the United States.

An additional factor that weighs in favor of exclusion is the inaction by law enforcement in the three years between the time the TECS report on Robinson was created and he was stopped at JFK airport. There is no indication that after generating the purportedly reliable information that led to the TECS lookout on Robinson in November 2019, law enforcement took any steps to act on it. As noted *supra*, every download, every purchase, and every viewing of child pornography causes harm to the victims who were forced to participate in its creation, and to society as a whole. And yet, after learning that Robinson may have been linked to the unlawful purchase of child pornography, it appears that neither NTC nor any other law enforcement agency took any steps to confirm that fact and seize any CSAM he may have downloaded. They did not knock on his door and attempt to interview

him about these suspicious purchase(s). They did not seek a warrant that could have led to Robinson's arrest in 2019. They did not ask if he would be willing to cooperate in a broader effort to identify the source of CSAM he illegally purchased — which could have led them to others far more directly engaged in "[t]he trade of child pornography[,] . . . a particularly vile aspect of the Internet." *Raymonda*, 780 F.3d at 120. Instead, they simply waited three years for a man who had never once left the country to go on his first trip overseas, then used the dragnet of the border search exception to compel him to surrender and provide the passcodes for the electronic devices in his possession.

The Court need not decide whether this was due to mere inertia, or a more deliberate effort "to shirk the warrant requirement that would otherwise apply to searches of cellphones for evidence of a domestic crime by directing the seizure of the phone at the airport." *Fox*, 2024 WL 3520767, at *10. But given the significant quantity of CSAM that was eventually found on Robinson's devices, the fact that the government waited three years to rely on its claimed border search authority rather than timely acting on an investigative lead likely increased the harm caused by having this material in circulation. In assessing the deterrence value of exclusion, then, the Court finds that strict application of the exclusionary rule in Robinson's case may incentivize law enforcement to take prompt action when they identify a potential purchaser of child pornography, rather than waiting years for that person to leave the country.

Thus, for the reasons discussed above, the Court finds that the good faith

exception does not apply to the initial search of Robinson's iPhone at JFK airport on November 14, 2022, and that the "corrective value" of deterrence outweighs the societal cost of excluding the seized evidence here. *Raymonda*, 780 F.3d at 117–18.

**C. Forensic Search: Reliance on Warrant**

The government further argues that the fruits of HSI's subsequent forensic search of that device should not be suppressed because it was conducted by Agent Stepien pursuant to a warrant. *See* Gov't Opp at 25.

As a preliminary matter, there is no dispute that the evidence obtained from the manual search of Robinson's phone at JFK Airport (namely, the fact that agents viewed "at least five" photographs that appeared to depict CSAM, Warrant Aff. ¶¶ 7–8) is what provided the agents with probable cause to obtain the warrant. However, even if a search warrant affidavit relies in part on what a court later concludes was illegally obtained evidence (as the Court has here), if "the remaining [untainted] portions of the affidavit would support probable cause, the warrant was properly issued." *United States v. Trzaska*, 111 F.3d 1019, 1028 (2d Cir. 1997). Here, there is no colorable argument that Magistrate Judge Cho had probable cause to issue the warrant without considering the information provided by Agent Stepien about the identification of apparent CSAM on Robinson's phone by Officer Nunes and then Agent Anstee when they manually searched the device. *See* Warrant Affidavit at 2–3. Thus, had the tainted evidence been excised from Agent Stepien's search warrant affidavit, probable cause would not have existed to issue the warrant.

But this is not the end of the analysis. When probable cause depends on

tainted information, the Court must determine if the "agent who conducted the search acted in good faith reliance on the search warrant." *United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985). "[W]here a search is conducted pursuant to a judicially authorized warrant, a presumption of validity obtains with respect to the affidavit supporting the search warrant." *Lauria*, 70 F.4th at 124 (internal quotation marks omitted).

Thus, because Agent Stepien acted pursuant to a judicially authorized search warrant, his search is cloaked in a presumption of good faith. However, that cloak falls away when an officer "knows, or has reason to know, that he has materially misled a magistrate on the basis for a finding of probable cause." *Golino v. City of New Haven*, 950 F.2d 864, 871 (2d Cir. 1991). And "[w]hen the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144).

The Second Circuit has identified at least four circumstances where an officer's "reliance on an invalid warrant is unreasonable." *In re 650 Fifth Ave. & Related Properties*, 934 F.3d 147, 162 (2d Cir. 2019). At issue in this case is the circumstance "where the issuing magistrate has been knowingly misled." *Id.* (quoting *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011)). When the challenge to a warrant affidavit is not that it contained what turned out to be erroneous factual information — but rather that law enforcement's actions were themselves in violation of the Fourth Amendment — the Court must determine if law enforcement acted knowingly

or recklessly in preparing the affidavit. *See United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.), *on reh'g*, 91 F.3d 331 (2d Cir. 1996). Specifically, the Court must determine whether the agent provided the issuing magistrate with enough information to "decide whether [law enforcement's] conduct was sufficiently illegal and in bad faith to preclude a valid warrant." *Id.* Moreover, "[t]he burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance" on a subsequently invalid warrant. *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992).

This means that even if the facts cited in support of probable cause in a warrant affidavit were the product of what was later deemed to be an illegal search, if the law enforcement officer brought all relevant information and circumstances surrounding the search to the magistrate judge, "[t]here is nothing more the officer could have or should have done," and suppression is inappropriate. *Thomas*, 757 F.2d at 1368. In *Thomas*, the Second Circuit found that a canine sniff at the defendant's door, which led to the discovery of incriminating evidence, was unconstitutional. *Id.* at 1366–68. However, the Circuit determined that because "the DEA agent brought this evidence, *including the positive 'alert' from the canine*, to a neutral and detached magistrate," and the magistrate determined there was probable cause for the warrant, "it was reasonable for the officer to rely on this determination." *Id.* at 1368 (emphasis supplied).

On the other hand, if the affidavit in support of a warrant application does not allow the issuing judge to "make a valid assessment of the legality of the warrant

that he [is] asked to issue," the good faith exception will not apply. *Reilly*, 76 F.3d at 1280. In *Reilly*, officers had illegally entered the curtilage of the defendant's property in order to obtain the evidence (marijuana plants) that supported probable cause. *Id.* at 1279. The Second Circuit found that because the concept of curtilage was clearly protected in Fourth Amendment jurisprudence at the time, "the officers undertook a search that caused them to invade what they could not fail to have known was potentially [defendant's] curtilage. *They then failed to provide [the issuing judge] with an account of what they did.*" *Id.* at 1281 (emphasis supplied). Instead, the warrant affidavit "presented only a bare-bones description" of the premises, which "was almost calculated to mislead." *Id.* at 1280. The Circuit held that because the issuing magistrate judge did not have "crucial" facts to determine if the pre-warrant search was legal, it was "the officers . . . themselves [who were] ultimately responsible for the defects in the warrant." *Id.* at 1280–81. Thus, the "the good faith exception does not apply when officers do not provide an issuing judge with details about their conduct during a pre-warrant search." *Id.* at 1280.

*Thomas* and *Reilly* provide this Court with key guideposts in assessing whether the government has met its burden of proving that Agent Stepien's reliance on the warrant is covered by the good faith exception. More recently, sitting *en banc*, the Second Circuit provided a roadmap as to how to determine if a situation is more akin to *Reilly* or *Thomas*. The Circuit indicated that a court must ask if agents "disclosed all crucial facts for the legal determination in question to the magistrate judge," then, a court must determine whether the agents preparing the affidavit had

"significant reason to believe that their predicate act was . . . unconstitutional." *Ganias*, 824 F.3d at 223 (internal quotation marks omitted); *see also id.* at 224 (finding that agent who "provided sufficient information in her affidavit to apprise the magistrate judge of the pertinent facts regarding . . . the alleged constitutional violation on which [Ganias] relies" was covered by good faith exception). In *Fox*, Judge Garaufis helpfully summarized these key components as "materiality (whether [the agent] materially misled the magistrate) and knowledge (whether [the agent] made these omissions knowingly, recklessly or with gross negligence)." 2024 WL 3520767, at *22.

Turning to Agent Stepien's warrant application, he described the events leading to the CBP and HSI searches of Robinson's phone only as follows:

> [] On November 14, 2022, ROBINSON landed at John F. Kennedy International Airport ("JFK Airport"), traveling from Cairo, Egypt, via British Airways flight BA 115 arriving from London, United Kingdom. He was stopped by United States Customs and Border Protection ("CBP") at JFK Airport for secondary inspection. A border search was conducted. During the search, ROBINSON voluntarily gave CBP officers the password for the Subject Device. Upon manually reviewing the Subject Device, CBP officers identified that there was child sexual abuse material on the subject device.
>
> [] At the border, a law enforcement agent with HSI conducted a preliminary review of the Subject Device and confirmed that it contained at least five photos containing child sex abuse material. Specifically, the law enforcement agent with HSI reviewed several images of what appeared to be a minor male, approximately age 13 to 16 years old, engaged in sexual activity, including anal sex and oral sex, with an adult male. There were also several images of the minor male naked, as well as close-up images of the minor male's genitalia.

Warrant Aff. ¶¶ 7–8 (footnotes omitted).

After the sentence, "A border search was conducted[,]" Agent Stepien added a

footnote, which read:

> The federal government has "broad plenary powers to conduct so-called 'routine' searches at the border even without 'reasonable suspicion that the prospective entrant has committed a crime.'" *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015) (quoting *Tabbaa v. Chertoff*, 509 F.3d 89, 97–98 (2d Cir. 2007))

*Id.* at 3 n.1.

What Agent Stepien notably omitted from the search warrant affidavit, of course, was any mention of the November 2019 TECS hit: *i.e.,* the very reason why Robinson was referred to secondary inspection to have his devices searched. This was not because Agent Stepien was ignorant of that fact: at the suppression hearing, he confirmed that at the time he applied for the warrant, he was fully aware that the reason Robinson had been referred to secondary inspection was because Nunes was alerted to this TECS hit. *See* Hr'g Tr. at 146. And of course, the TECS hit is the very information that the government now relies upon to contend that the initial search of Robinson's iPhone was supported by reasonable suspicion. Additionally, Agent Stepien informed the magistrate judge that Robinson "voluntarily" provided the passcode to his phone, Warrant Aff. ¶ 7, while omitting the fact that he was provided with a tear sheet essentially telling him that CBP had full authority to compel him to submit to that search. *See* Tear Sheet at 2 (stating that "[a]ll persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention" and that Robinson was "receiving this sheet because [his] electronic device(s) have been detained for further examination").

Like the officers in *Reilly*, Agent Stepien was fully aware of the factual context

surrounding the original search, but he provided only a "bare-bones" recitation of those facts. And as in *Reilly,* he did so despite being aware of the potential Fourth Amendment implications of the facts he omitted — *i.e.,* that established caselaw distinguishes between "routine" and "nonroutine" searches, and limits the circumstances under which border agents may conduct a search that falls into the latter category. By citing to the Second Circuit case *Levy* for general propositions of law regarding "routine" border searches, and describing the search only in generic, passive-voice terminology, *see* Warrant Aff. ¶ 7 ("A border search was conducted."), Agent Stepien falsely indicated to the magistrate judge that what occurred was nothing more than a routine, suspicionless search of a randomly selected traveler.

At oral argument, the government contended that Agent Stepien had no reason to include the information regarding the TECS hit as he believed that it was a routine border search, and because no level of suspicion is necessary for a routine border search, including the TECS hit was unnecessary. *See* Oral Arg. at 64 (argument, by government counsel, that Stepien did not mention the TECS hit because "it's not necessary to include all the background about investigation when making a warrant application"); *see also id.* at 67 ("[I]t is outside the practice of search warrant drafting to include every single fact that might have led to the recovery of an electronic device that is now the subject of a search warrant."); *see also id.* at 66 ("It's impossible to include every single thing that happens in an interaction with somebody when you're writing a search warrant affidavit.").

The government is correct that an officer need not provide every detail of an

earlier search in a warrant affidavit. However, it has been settled law in this Circuit for nearly three decades that an officer must provide *relevant* "details about their conduct during a pre-warrant search." *Reilly*, 76 F.3d at 1280. That is particularly so where — as here — the affiant is aware of existing Fourth Amendment caselaw concerning the specific category of searches that the magistrate judge may need to apply to assess the constitutionality of the officers' earlier actions. *Id.* at 1281 (finding officers' actions were not protected by good faith when they "undertook a search that caused them to invade what they could not fail to have known was potentially [defendant's] curtilage" and "their actions in not describing [the search] to the judge [is not] the kind of behavior to which the term good faith can be applied"). The record before this Court, including but not limited to its assessment of Agent Stepien's demeanor at the hearing, leads this Court to the firm conclusion that the omission of the TECS hit from the warrant affidavit was not inadvertent. It is difficult to conceive how any officer acting in good faith could omit that information inadvertently, or (as the government now contends) do so in order to limit the affidavit to only necessary "context." And it is a particularly difficult claim to credit here, since Agent Stepien included other far less relevant (or irrelevant) information, such as the airline and flight number for the plane on which Robinson arrived at JFK. *See* Warrant Aff. ¶ 7.

Notably, at the hearing, the government did not elicit from Agent Stepien any explanation as to why he did not simply inform Magistrate Judge Cho that a TECS hit stating that Robinson was linked to the purchase of CSAM three years prior was

the actual reason for the search. He simply agreed with the general questions from the government that he believed the observations made during the search of the phone "were lawfully obtained" because the search was a "border search." Hr'g Tr. at 150.

Additionally, even if the Court were to credit Agent Stepien's claim that he believed this was a "routine" border search requiring no reasonable suspicion, that does not explain why he would have left the TECS report out of the affidavit — unless he did not want the issuing judge to ask questions regarding the TECS hit, its origins, its age, and anything else that might bear on whether the agents had reasonable suspicion to search Robinson's phone at the border. If Agent Stepien sought the warrant not to sanitize the earlier warrantless search, but in a good faith effort to ensure that HSI had probable cause to conduct a forensic search, he would have certainly included the details that provided law enforcement with particularized grounds to search the phone. The Court does not come to this view out of conjecture; it does so based on Agent Stepien's own words. In the warrant affidavit, Agent Stepien wrote that "while HSI might already have all necessary authority to examine the Subject Device, I seek this additional warrant *out of an abundance of caution* to be certain that an examination of the Subject Device will comply with the Fourth Amendment." Warrant Aff. ¶ 10 (emphasis supplied). It defies common sense that Agent Stepien would prepare an entire search warrant affidavit to ensure the legality of a device search "out of an abundance of caution," but would not include key details in that affidavit that, in the government's own view, provided particularized

suspicion that Robinson had contraband on that device when he reentered the country.

Thus, in light of the foregoing record, the Court finds that Agent Stepien knowingly and intentionally omitted what he knew or should have known was material information regarding the TECS report that led to the manual search of Robinson's phone. Moreover, he falsely implied, through the statements he did include in the affidavit, that the search at issue was merely a "routine search[] at the border" of a randomly selected traveler. Warrant Aff. at 3 n.1 (internal quotation marks omitted). It would not be unreasonable to conclude that Agent Stepien did so with the specific intent to mislead the magistrate judge — *i.e.,* because he did not want Judge Cho questioning whether the initial search of Robinson's phone was routine or nonroutine, and whether it was supported by reasonable suspicion. But at the very least, it is clear that Agent Stepien acted recklessly when he presented the court with this incomplete and misleading warrant affidavit. *See Reilly*, 76 F.3d at 1280 ("We have previously held that recklessness may be inferred when omitted information was clearly critical to assessing the legality of a search." (internal quotation marks omitted)).

It is not only what Agent Stepien left out of his affidavit that leads this Court to conclude that he did not act in good faith; it is also the information he included. Agent Stepien wrote that Robinson "voluntarily gave CBP officers the password" for his phone. Warrant Aff. ¶ 7. This strongly implied that, even if the search was not valid under the border exception, it was a "consent search." While that is a well-

recognized exception to the warrant requirement, a search is not voluntary if "granted only in submission to lawful authority." *Schneckloth v. Bustamonte*, 412 U.S. 218, 233 (1973); *see also United States v. Isiofia*, 370 F.3d 226, 230 (2d Cir. 2004) ("The government has the burden of proving, by a preponderance of the evidence, that a consent to search was voluntary."). Here, through taking Robinson into a secondary inspection area from which he was not free to leave, providing him with a tear sheet which indicated that CBP had full legal authority to search his phone, and stating, "what's the password for the phone," Hr'g Tr. at 55, Officer Nunes did not ask Robinson for his consent to examine the contents of his cell phone; she did not give Robinson any option but to consent to that search.

The government has, appropriately, not argued that this was in fact a consent search. Rather, it argues that the statement that Robinson "voluntarily gave CBP officers [his] password" in the warrant affidavit did not imply or suggest that it was a consent search; instead, it argues that Agent Stepien included this language merely to provide "context as to how this came to be a search at all." Oral Arg. Tr. at 30–31.

This argument is implausible. The warrant affidavit contains only five sentences detailing all the events that took place from when Robinson landed at JFK to when CBP officers identified CSAM on his phone. *See* Warrant Aff. ¶ 7. This Court fails to understand how the sentence that "Robinson voluntarily gave CBP officers the password for the Subject Device" was more relevant "context" than the very reason Officer Nunes testified that she was mandated by CBP policy to take Robinson to secondary screening and search his devices. When so little other information about

the search was provided, it is a fair inference that this information was included to falsely imply that the search was performed only because Robinson "voluntarily" consented to it.

For the foregoing reasons, this Court finds that Agent Stepien's material omissions from — and misrepresentations in — his warrant affidavit amounted to, at the very least, a "reckless disregard for the truth." *Lauria*, 70 F.4th at 125 (quoting *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000)). Thus, his subsequent reliance on the search warrant is not protected by the good faith exception, and the evidence obtained from the forensic search of Robinson's iPhone following execution of the search warrant must be excluded.

## CONCLUSION

As the initial search of Robinson's iPhone was conducted without a warrant and probable cause, it violated his Fourth Amendment right to be free from unreasonable search and seizure. Further, as the government has not shown that the officers who conducted the search had an objective, good faith basis to believe that their conduct was lawful under binding appellate precedent, all the evidence obtained from that search must be excluded. Nor can the government rely upon evidence obtained from the subsequent judicial warrant, as the HSI agent who submitted the warrant affidavit knowingly failed to disclose to the magistrate judge the circumstances surrounding the earlier search of Robinson's phone, and exhibited what the Court concludes was, at the very least, a reckless disregard for the truth.

The Court does not come to this conclusion lightly. Robinson's cell phone contained a substantial quantity of child pornography, the circulation and possession of which caused enormous harm to the minors depicted in those images. But "[o]ur commitment to equal justice and the rule of law requires the courts to faithfully apply criminal laws as written . . . even when the conduct alleged is indisputably abhorrent." *Fischer v. United States*, 603 U.S. 480, 499 (2024) (Jackson, J., concurring). Certainly, no less is required when courts are called upon to faithfully apply the Fourth Amendment's guarantees.

For these reasons, Robinson's motion to suppress the evidence recovered from his iPhone is GRANTED.

SO ORDERED.

*/s/ Nina R. Morrison*
NINA R. MORRISON
United States District Judge

Dated: May 9, 2025
Brooklyn, New York